

CLAIMS

What is claimed is:

1. A communication authorization method, comprising the steps of:
- 5 receiving a request for access information to access content;
- generating the access information to access the desired content from a first application server;
- generating authentication of the access information using a first service ticket;
- and
- 10 sending the access information and authentication to a client.
2. The method as claimed in claim 1, wherein the step of generating authentication including generating a third party server signature using the first service ticket, wherein the first service ticket is a third party server service ticket to
- 15 the first application server.
3. The method as claimed in claim 1, wherein the step of generating the access information including generating session rights and encrypting at least a portion of the session rights using a third party server service key for the first
- 20 application server.
4. The method as claimed in claim 1, further comprising the step of:
- encrypting at least a portion of the authentication using the first service ticket.
5. The method as claimed in claim 4, further comprising the steps of:
- 25

requesting a ticket granting ticket (TGT ticket);
 receiving a TGT ticket;
 requesting the third party server service ticket for the first application server;
 5 and
 receiving the third party server service ticket for the first application server.

6. The method as claimed in claim 1, further comprising the steps of:
 receiving a key request including the access information and authentication;
 10 extracting the access information and authentication;
 verifying the authentication of the access information using the first service
 ticket, and client authorization; and
 issuing a key reply if the authentication of the access information and client
 authorization are verified.

7. The method as claimed in claim 6, further comprising the steps of:
 a client generating a key request including the access information and the
 authentication;
 sending the key request to the first application server; and
 20 receiving the key reply (KEY_REP) if the authentication of the access
 information and client authorization are verified by the first application server.

8. A method for verifying authorization for a client to gain access to
 content and/or services, comprising the steps of:
 25 receiving a key request;

extracting third party server access information and third party server authentication from the key request;

5 verifying an authentication of the third party access information and a client authorization; and

issuing a key reply if the authentication of the third party access information and the client authorization are verified.

9. The method as claimed in claim 8, further comprising the step of
10 authenticating the third party server access information using the third party server authentication.

10. The method as claimed in claim 9, wherein the step of authenticating
15 includes extracting a first service ticket from the authentication and authenticating the third party server access information using the first service ticket.

11. The method as claimed in claim 8, wherein the step of extracting the
third party server authentication, further comprising the steps of extracting a session
key from the key request; and
20 the step of authenticating the access information including verifying a third party server signature using the session key.

12. The method as claimed in claim 11, wherein the step of extracting the
session key including decrypting at least a portion of the key request using an
25 application server service key and extracting the session key.

13. The method as claimed in claim 8, further comprising the steps of:
 receiving a request for the access information to access content;
 generating the third party server access information to access the desired
 5 content from a first application server; and
 generating the third party server authentication of the access information.

14. The method as claimed in claim 13, wherein the step of generating the
 third party server authentication including incorporating a third party server service
 10 ticket for the first application server.

15. The method as claimed in claim 14, wherein the step of generating the
 authentication including generating a signature utilizing a session key of the third
 party server service ticket.

16. The method as claimed in claim 14, wherein the steps of verifying the
 authentication of the access information including extracting the third party server
 service ticket and verifying the third party server service ticket.

17. A method for providing secure communication when distributing
 services, comprising the steps of:
 receiving a selection for services;
 issuing access information for the services;
 issuing authentication of the access information;
 25 receiving a key request;

verifying an authentication of the access information and a client authorization
utilizing, at least in part, a first service ticket; and

issuing a key reply to a client if the authentication of the access information
5 and the client authorization are verified.

18. The method as claimed in claim 17, further comprising the steps of:
receiving a first service ticket request from a third party server for a first
server;

10 issuing the first service ticket to the third party server for the first server; and
the steps of issuing access information and authentication including generating
the access information and authentication using the first service ticket.

19. The method as claimed in claim 17, further comprising the steps of:
15 receiving a second service ticket request for the first server;
issuing a second service ticket for the first server; and
the step of receiving a key request wherein the key request includes the second
service ticket.

20. The method as claimed in claim 17, wherein:
the step of verifying the authentication of the access information including:

extracting the first service ticket;
decrypting the first service ticket;
extracting a session key from the first service ticket;
25 generating a signature using the session key; and

verifying the signature with the authentication.